PATENT APPLICATION

ELECTRONIC AUTHENTICATION METHOD, ELECTRONIC AUTHENTICATION APPARATUS AND ELECTRONIC AUTHENTICATION STORAGE MEDIUM

Inventors: **Junichi Miura**
Tokyo, Japan
Citizenship: Japan

Yukio Saito
Narashino, Japan
Citizenship: Japan

Ryota Koiso
Kawaguchi, Japan
Citizenship: Japan

Assignees: **Hitachi, Ltd.**
6, Kanda Surugadai 4-chome
Chiyoda-ku, Japan
Incorporation: Japan

Entity: Large

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, California 94111-3834
(415) 576-0200

PATENT
16869P-008100
349900460US1

ELECTRONIC AUTHENTICATION METHOD, ELECTRONIC AUTHENTICATION APPARATUS AND ELECTRONIC AUTHENTICATION STORAGE MEDIUM

CROSS-REFERENCES TO RELATED APPLICATIONS

This application claims priority from Japanese Patent Application Reference No. 11-174066, filed June 21, 1999.

BACKGROUND OF THE INVENTION

The present invention relates to a system for transmitting contents from an information processing apparatus rendering services to an information processing apparatus making a request for a service and transmitting input data for the contents from the latter information processing apparatus to the former information processing apparatus. More particularly, the present invention relates to an electronic authentication techniques for authenticating legitimacy of input data for a content access.

In the field of electronic business transactions using the Internet, security technologies such as authentication of a true person and prevention of data falsification have become increasingly important. As conventional security technologies, a variety of efforts have been made such as establishment of a password system, establishment of a variety of encryption systems for encrypting data and issuance of an electronic note of authentication.

What is really needed are techniques for verifying that the correct response data is provided responsive to an access request for contents in a system in which a server transmits the requested contents to a client requestor and the client transmits input data to the server as the response data responsive to the contents.

SUMMARY OF THE INVENTION

According to the invention, techniques for verifying that data input as a response to presented contents is true input data for a content access are provided. In

specific embodiment[redacted] present invention can provide meth[redacted], systems and storage media that store a program, each of which implement electronic authentication techniques.

In a representative embodiment according to the present invention, there is provided an electronic authentication method that comprises a variety of steps, such as a step of generating an identifier for contents in a first information processing apparatus and storing the identifier in a storage unit. Transmitting the contents and the identifier to a second information processing apparatus can also be part of the method. Steps of inputting data for the contents in the second information processing apparatus and transmitting the input data and the identifier from the second information apparatus to the first information apparatus can also be included in the method. Further, the method can also include authenticating legitimacy of the input data and invalidating the stored identifier if the received identifier matches the identifier in the storage unit in the first information processing apparatus.

In addition, the present invention relates to a first information processing apparatus and a second information processing apparatus which are used for implementing the method described above. Furthermore, the present invention characterizes a storage medium for storing a program implementing the electronic authentication described above.

In a representative embodiment according to the present invention, a WWW server program generates an identifier for an access to contents and catalogs the identifier in an access control table. The WWW server program then embeds the identifier in the contents before transmitting the contents to a client. A WWW browser program displays the contents and adds an access number fetched from the contents to input data for the contents. The WWW browser program then transmits the input data to a WWW server. If the identifier added to the input data received from the WWW browser program matches an identifier cataloged in the access control table, the WWW server program authenticates the legitimacy of the input data and deletes the cataloged identifier.

Numerous benefits are achieved by way of the present invention over conventional techniques. The present invention can provide a method to verify that data input as a response to presented contents is true input data for a content access. The present invention can provide a storage medium for storing a program implementing such

an electronic authentication method. When personal information, transaction data and the like are transmitted from the client 1 to the WWW server 2 in response to contents transmitted from the WWW server 2 to the client 1 in a transaction such as Internet shopping or an electronic business transaction using the Internet, the present invention allows the personal information, the transaction data and the like to be verified as input data for a legal access to the contents. In addition, the present invention is also capable of preventing double transaction data from being transmitted by issuing two or more orders for one order form by user's mistake.

These and other benefits are described throughout the present specification. A further understanding of the nature and advantages of the invention herein may be realized by reference to the remaining portions of the specification and the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates a diagram showing the configuration of a system for rendering services by using the Internet as implemented by an embodiment of the present invention;

Fig. 2 illustrates a diagram showing the data format of an access information record stored in an access control table 28 according to a particular embodiment of the present invention;

Fig. 3 illustrates a flowchart showing the flow of processing carried out by the system implemented by a particular embodiment of the present invention;

Fig. 4 illustrates a continuation flowchart of the one of Fig. 3 showing the flow of processing carried out by the system implemented by a particular embodiment of the present invention;

Fig. 5 illustrates a diagram showing the hardware configuration of a WWW server employed in a particular embodiment of the present invention; and

Fig. 6 illustrates a diagram showing the hardware configuration of a client employed in a particular embodiment of the present invention.

DESCRIPTION OF THE SPECIFIC EMBODIMENTS

The present invention provides techniques for verifying that data input as a response to presented contents is true input data for a content access. In specific

embodiments, the present invention can provide methods, systems and storage media that store a program, each of which implement electronic authentication techniques.

Techniques for authenticating a true person by an electronic signature include encrypting transmitted data by using a private key. With such techniques, however, it is often necessary to control the private key on the transmitter side. As a result, control can become complicated. In addition, in the case of authentication of a true person by using an ID or a password, the password may be transmitted through a network as a clear text, raising a problem of inability to prevent falsification of the identity of a true person by another illegally using a password intercepted during transmission. For a more detailed description of techniques for authenticating a person by an electronic signature used in encrypting transmitted data by using a private key, further reference may be had to a Japanese Patent Laid-open No. Hei 10-32570, the entire content of which is incorporated herein by reference for all purposes.

In systems using the Internet, a client generally transmits a request for contents to a WWW (World Wide Web) server. In response to this request, the WWW server transmits the requested contents to the client, which then displays the contents on a display unit. When the client inputs data for the contents and transmits the input data to the WWW server, the WWW server processes the data received from the client. The client is capable of copying the contents with ease. Thus, it is quite within the bounds of possibility that an illegal operation is carried out on copied contents. For example, a copy of the contents is extracted and reused, or another user falsifies data through a content screen and transmits the falsified data to the WWW server.

Embodiments according to the present invention that can overcome many such limitations of conventional methods will now be described by referring to diagrams as follows.

Fig. 1 is a diagram showing the configuration of a system for rendering services by using the Internet as implemented by a specific embodiment. As shown in Fig. 1, the system comprises a client 1, a WWW server 2 and the Internet 3 which serves as a network connecting the client 1 and the WWW server 2 to each other.

As shown in Fig. 5, the hardware configuration of the WWW server 2 comprises a storage unit 21, a central processing unit (CPU) 22, a communication-network interface 23, a content-DB interface 24, an access-control-table interface 26 and

a temporary storage [redacted] (memory) for storing a WWW server [redacted]gram 25 which are connected to each other by a bus 27.

Storage unit 21 is used for permanently storing programs and data used in the WWW server 2. The storage unit 21 is implemented typically by a hard disc and a floppy disc. The CPU 22 executes overall control of the components composing the WWW server 2 and carries out processing. The communication-network interface 23 is an interface for handling exchanges of data with the client 1 by way of the Internet 3. The content-DB interface 24 is an interface for handling exchanges of data with a content DB 29 of Fig. 1. The access-control-table interface 26 is an interface for handling exchanges of data with an access control table 28 of Fig. 1. The memory is used for storing a WWW server program 25 and other information which are required in the processing carried out by the CPU 22.

As shown in Fig. 6, the hardware configuration of the client 1 comprises a display unit 11, an input unit 12, a communication-network interface 13, a temporary storage unit (memory) for storing a WWW browser program 16, a central processing unit (CPU) 14 and a storage unit 15 which are connected to each other by a bus 17.

Display unit 11 is used for displaying a message and other information to the user utilizing the client 1. The display unit 11 is implemented typically by a liquid-crystal display device or a CRT. Input unit 12 is used by the user for entering data, an electronic message and other information, for example. The input unit 12 is implemented by components such as a keyboard and a mouse. The communication-network interface 13 is an interface for handling exchanges of data with the WWW server 2 by way of the Internet 3. Storage unit 15 is used for permanently storing programs and data used in the client 1. The storage unit 15 is implemented typically by a hard disc and a floppy disc. The CPU 14 executes overall control of the components comprising the client 1 and carries out processing. The memory is used for storing the WWW browser program 16 and other information which are required in the processing carried out by the CPU 14.

The WWW browser program 16 transmits a request for contents to the WWW server 2 by way of the Internet 3 and displays the contents received from the WWW server 2 on the display unit 11. In addition, the WWW browser program 16 also transmits data entered via the input unit 12 to the WWW server 2.

The WWW server 2 is a computer on the service rendering side. The storage unit connected to the processing unit is used for storing the access control table 28

and the content DB (database) 29. The access control table 28 is used for storing authentication information for controlling accesses to contents. The content DB 29 is a DB for storing contents to be presented to the client 1. Contents are display screen information stored in the WWW server 2 to be presented to the client 1. Contents can include text data, image data, a still picture or a moving picture. The WWW server program 25 is stored in the memory employed in the WWW server 2 and is executed by the processing unit of WWW server 2. WWW server program 25 transmits contents to the client 1 in accordance with a request made by the client 1. In addition, the WWW server program 25 stores authentication information in the access control table 28 for each request for contents and authenticates data received from the client 1, which is relevant to the contents.

It should be noted that the WWW server program 25 includes an electronic authentication function according to the present invention. WWW server program 25 is stored in a storage medium and then transferred to the memory employed in the WWW server 2 through a drive unit also employed in the WWW server 2 for execution by the processing unit of the WWW server 2. As an alternative, the WWW server program 25 is received by the WWW server 2 from the network and then stored into the memory of the WWW server 2 to be executed by the processing unit employed in the WWW server 2. The WWW browser program 16 includes an electronic authentication function according to the present invention. The WWW browser program 16 is stored in a storage medium and then transferred to the memory employed in the client 1 through a drive unit also employed in the client 1 for execution by the processing unit of the client 1. As an alternative, the WWW browser program 16 is received by the client 1 from the network and then stored into the memory of the client 1 to be executed by the processing unit employed in the client 1.

Fig. 2 is a diagram showing the data format of each access information record stored in the access control table 28. As shown in the figure, the record comprises an access number 41, a public key 42, a private key 43 and a cataloging date and time 44. The access number 41 is created for each access to contents and associated with the access to the contents. The public key 42 is an encryption key generated for protecting the confidentiality of data received from the client 1. The private key 43 is a decryption key for decrypting an encrypted text obtained as a result of encryption using the public

key 42. Much like t[redacted]ccess number 41, the public key 42 a[redacted]he private key 43 are generated for each access to contents.

The cataloging date and time 44 is a date and a time at which the access information record is cataloged in the access control table 28.

Figs. 3 and 4 illustrate a flowchart showing the flow of processing carried out by execution of the WWW browser program 16 stored in the client 1 and the WWW server program 25 stored in the WWW server 2. As shown in Fig. 3, the flowchart begins with a step 51 at which the WWW browser program 16 transmits a request for contents to the WWW server 2. Then, at a step 52, the WWW server program 25 receives the request for contents. Subsequently, at a step 53, a random number is generated to be used as an access number. Then, at a step 54, a public key and a corresponding private key are generated in accordance with a public key encryption system. Subsequently, at a step 55, the content DB 29 is searched for the requested contents. Then, at a step 56, the access number generated at the step 53 and the public key generated at the step 54 are embedded in the contents by using a digital watermark technology for making the key invisible to the user. As a position of the contents at which these pieces of information are embedded, it is desirable to provide a rectangular area including a specific mark such as an Internet mark or a logo mark in order to make positioning convenient. In addition, it is desirable to embed the information in a concentrated picture area in order to make the digital watermark technology easy to apply. Subsequently, at a step 57, the access number 41 generated at the step 53, the public key 42 and the private key 43 generated at the step 54 and an additional cataloging date and time 44 are cataloged in the access control table 28 as a new access information record. Then, at a step 58, the contents including the authentication information embedded therein as described above are transmitted to the client 1.

Subsequently, the WWW browser program 16 receives the contents at a step 59 and displays them on the display unit 11 at a step 60. While the displayed contents are visible to the user, the access number and the public key embedded in the contents are not displayed so that the user is not capable of recognizing the number and the key visually. As a representative example of contents, the contents can include image information of items in a catalogue for an electronic commerce application, from which a user can select a favorite item.

Then, at a step 61, when data such as personal information, typically including an address to which a product is to be delivered is entered via the input unit 12, the flow of the processing continues as illustrated by the flowchart shown in Fig. 4. As shown in the figure, the flowchart begins with a step 62 at which the WWW browser program 16 identifies the position of the embedded digital watermark on the contents and fetches the embedded access number and the embedded public key. Then, at a step 63, the input data is encrypted by using the public key to create an electronic message. Subsequently, at a step 64, the access number is added to the electronic message which is then transmitted to the WWW server 2 along with the access number. Even though the access number can also be encrypted, such encryption is not required since its degree of confidentiality is low.

Subsequently, the WWW server program 25 receives this electronic message at a step 65 and searches the access control table 28 for a record indicated by the access number included in the electronic message at a step 66. Then, the result of the search is examined at a step 67 and, if the outcome of the examination carried out at the step 67 is YES, indicating that the access information record was found, the server program authenticates the legitimacy of access, and the processing continues at a step 68. At step 68, an encrypted portion of the electronic message is decrypted by using the private key. Otherwise, if the outcome of the examination carried out at the step 67 is NO, indicating that the access information record was not found, the processing continues at a step 69, at which the received electronic message is discarded. From the step 68, the flow of the processing proceeds to a step 70 to form a judgment as to whether or not the encrypted portion of the electronic message could be decrypted into data with a meaning expected in advance. If the outcome of the judgment formed at the step 70 is YES, indicating that the encrypted portion could be decrypted, the processing continues to a step 71, at which the access information record is deleted from the access control table 28. Then, at a step 72, subsequent processing is carried out on the basis of the input data. In the case of electronic commerce applications, the inputted selection information can be transmitted to an Internet site where the item can be processed. Otherwise, if the outcome of the judgment formed at the step 70 is NO, indicating that the encrypted portion could not be decrypted, the flow of the processing continues to a step 73, at which the received electronic message is discarded. Then, at the step 74, the access information record is deleted from the access control table 28. Subsequent processing is not carried out.

Generally, the deleti[redacted] the access information record means [redacted]t the record is invalidated. In this example, access information is deleted from access control table 28. Alternatively, access number 41, its corresponding public key 42, secret key 43, and registering date and time 44, may have an effective flag, which can be set and reset according to whether the access information record is valid or invalid.

It is also worth noting that the WWW server 2 periodically checks the cataloging date and time 44 of each access information record cataloged in the access control table 28. In the event of a time-out where time of a predetermined length has lapsed since the time indicated by the cataloging date and time 44, the access information record is deleted from the access control table 28. In the case of a time-out, authentication of an access to contents accompanied by no response expressed by input data is halted. When access is not permitted, the display of client 1 can show that access has been denied because of an illegal access attempt. Such a display can provide to users an indication of a reason that access has been denied.

According to a specific embodiment described above, contents transmitted to the client 1 include an embedded access number which is generated for each access to contents. Thus, even if the contents are copied and data entered in response to the contents is transmitted to the WWW server 2, the access number will have already been invalidated by the WWW server 2, so that the data transmitted to the WWW server 2 will also be invalid. In addition, even if an access number is illegally intercepted in the course of the transmission of an electronic message from the client 1 to the WWW server 2 by way of the Internet 3, the access number will be invalidated in an attempt to reuse the number. In addition, even if the user of the client 1 is capable of decoding an access number embedded in contents, the number can not be reused for other purposes anyway.

In addition, according to a specific embodiment described above, a public key that can be used only once is embedded in contents transmitted to the client 1 to protect the confidentiality of data such as personal information transmitted from the client 1 to the WWW server 2. Thus, even if information encrypted by using the public key is illegally intercepted, it will be impossible to reuse the information. As a result, an unauthorized user is not capable of illegally intercepting personal information of another user in order to pretend to be the other user. It is also possible to avoid a wrongdoing such as falsification of information such as the amount of money or the quantity of products described on an order sheet.

As described above, the digital watermark technology is adopted in a specific embodiment. The adoption of the digital watermark technology can serve to conceal an access number and a public key by using a digital watermark technology since an access number and a public key are not substantive contents and, hence, do not have to be revealed to the user. Thus, there is especially no confidentiality in the digital watermark technology itself. Therefore, the digital watermark system can be widely applied to a large number of content packages. It is desirable to provide a system for embedding a watermark in a simple and reliable way so that the system can be applied as a common system to the WWW browser program 16 and the WWW server program 25.

In addition, in the embodiment described above, an access number is generated by the WWW server 2 as a random number. It should be noted, however, that an access number can also be generated as a serial number or a consecutive number so that the access number can be used for other purposes such as protection of the copyright of contents. If an access number is generated as a consecutive number, however, there is danger of an access number's being predicted in next generation of future contents on the basis of a result of decoding an access number embedded in present contents. As another alternative, a hash value is found from a number of digits in an access number by using a hash function, and the hash value of the access number is embedded in contents. In this case, the hash value is cataloged in the field for the access number 41 in an access information record and, at the step 66, the access control table 28 is searched for an access information record indicated by a hash number.

As described above, in a specific embodiment, response data is encrypted by using a public key which is generated along with an identifier of contents so as to prevent the response data from being intercepted illegally.

When personal information, transaction data and the like are transmitted from the client 1 to the WWW server 2 in response to contents transmitted from the WWW server 2 to the client 1 in a transaction such as Internet shopping or an electronic business transaction using the Internet, the present invention allows the personal information, the transaction data and the like to be verified as input data for a legal access to the contents. In addition, the present invention is also capable of preventing double transaction data from being transmitted by issuing two or more orders for one order form by user's mistake.

As described above, according to the present invention, a content identifier appended to contents transmitted by a server to a client accompanies data transmitted by the client to the server in response to the contents. Thus, transmission of data in response to contents in an access to the contents can be limited to one-time transmission to exclude disallowed response data using a copy of the contents and illegal response data intended to falsify information. As a result, the present invention is capable of proving that input data is correct data transmitted as a response to contents in an access to the contents. Although the above has generally described the present invention according to specific systems, the present invention has a much broader range of applicability.

The specific embodiments described herein are intended to be merely illustrative and not limiting of the many embodiments, variations, modifications, and alternatives achievable by one of ordinary skill in the art. Further, the diagrams used herein are merely illustrations and should not limit the scope of the claims herein. One of ordinary skill in the art would recognize other variations, modifications, and alternatives. Thus, it is intended that the foregoing description be given the broadest possible construction and be limited only by the following claims.

The preceding has been a description of the preferred embodiment of the invention. It will be appreciated that deviations and modifications can be made without departing from the scope of the invention, which is defined by the appended claims.